UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/803,167	03/16/2004	Robert N. Nazzal	12221-033001	4158

26161 7590 06/24/2008

FISH & RICHARDSON PC
P.O. BOX 1022
MINNEAPOLIS, MN 55440-1022

EXAMINER	
COLIN, CARL G	

ART UNIT	PAPER NUMBER
2136	

MAIL DATE	DELIVERY MODE
06/24/2008	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary	Application No.	Applicant(s)	
	10/803,167	NAZZAL, ROBERT N.	
	Examiner	Art Unit	
	CARL COLIN	2136	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE *3* MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *04 March 2008*.

2a)☒ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-22* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-22* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *04 March 2008* is/are: a)☒ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

Response to Arguments

1. In communications filed on 3/4/2008, applicant amends claims 1, 8, and 15. The following claims 1-22 are presented for examination.

1.1 In response to communications filed on 3/4/2008, the objection to the drawings has been withdrawn with respect to the amendment.

1.2 Applicant's arguments filed on 3/4/2008 have been fully considered but they are not persuasive. Regarding claim 8, applicant argues that determining the difference is not found on page 3, paragraphs 33 and 36 and paragraph 47. However, the rejection clearly states "further discloses a comparison is made between the two wherein the difference between them indicates suspicious network activity or abnormal activity (see page 1, paragraphs 11 and 15)" that meets the recitation of *determining whether there is a difference in the port protocols, by having a protocol that was in a current list but was not in the baseline list; and if there is a difference.* The limitation of indicating a new service involving the tracked entity is disclosed by Porras who discloses in paragraph 47 an example of discovery of a new service by examining traffic activity of a suspicious entity and once a threshold has been exceeded, the recent protocol (unknown port traffic may be compared to known port protocol (packets that have been collected over a period of time) indicating a new network service, which meets the claimed limitation. Regarding claim 9, Porras discloses in paragraph 47, the new service has been installed by the entity, and network

service using ports that are not authorized by an administrator, which meets the claimed limitation. Therefore, applicant has not overcome the 102 rejection of claims 8, 9, 11-13, 15, 16, and 18-21. With respect to claim 10, applicant argues that Porras does not disclose determining if the user is providing or using the new service. Examiner respectfully disagrees. Examiner respectfully disagrees as Porras discloses in paragraph 47, the new service has been installed by the entity, and network service using ports that are not authorized by an administrator. Paragraphs 45 and 48 further discloses monitoring and initiated login requests etc. With respect to claim 14, Examiner has provided applicant with prior art references for representing network events in a table. See, for instance, US 2003/0145225 to Bruton, III et al fig. 17 and paragraph 45. See US Patent 5,999,179 to Kekic, fig. 3 and US Patent 7,047,288 to Cooper et al. With regard to claim 1, Cooper discloses a field that depicts a range to track an entity by specifying for instance the policy domains, time domain or the monitoring points (see fig. 3, 5, 10C, fig. 21, and 31). Therefore, upon further consideration, applicant has not overcome the rejection of claim 1. In view of the above the claims remain rejected.

Claim Rejections - 35 USC § 102

2. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the

international application designated the United States and was published under Article 21(2) of such treaty in the English language.

Claims 8, 9, 11-13, 15, 16, and 18-21 are rejected under 35 U.S.C. 102(e) as being anticipated by US Patent Publication 2004/0010718 to **Porras et al**.

As per claim 8, **Porras et al** discloses a *method for detection of a new service involving an entity, the method comprises:* **Porras et al** discloses monitoring network activity of an entity (see page 1, paragraph 11) that meets the recitation of *entity being tracked,* which includes analyzing event records such as port protocols (see page 3, paragraph 31) the method includes collecting statistical measures that includes port protocols over a period of time comprising the most recent data represented as short-term statistical profiles (current list) and the normal, non-recent, data as long-term statistical profiles (baseline list) (see page 1, paragraphs 11 and 15, page 3, paragraphs 33 and 36 and page 4, paragraph 40) that meets the recitation of *retrieving a baseline list of port protocols used by a entity being tracked, the baseline value determined over a baseline period, retrieving a current list of port protocols for the entity being tracked;* and further discloses a comparison is made between the two wherein the difference between them indicates suspicious network activity or abnormal activity (see page 1, paragraphs 11 and 15) or indication of new service (see page 3, paragraphs 33 and 36 and page 4, paragraph 47) that meets the recitation of *determining whether there is a difference in the port protocols, by having a protocol that was in a current list but was not in the baseline list; and if there is a difference; indicating a new service involving the tracked entity.*

As per claim 9, **Porras et al** discloses *determining if the entity is providing or using the new service* (see page 3, paragraphs 33 and 36 and page 4, paragraph 47).

As per claim 11, **Porras et al** discloses *retrieving a value corresponding to the alert severity level set for violation of the rule* (see page 6, paragraph 67).

As per claim 12, **Porras et al** discloses *wherein the entity is at least one of a specific host, any host in a specific role, any host in a specific segment, or any host* ((see page 1, paragraph 10).

As per claim 13, **Porras et al** discloses *wherein the extent of the comparison is configured to for that host, in its role, in its segment or anywhere in the network* (see page 1. paragraph 7).

As per claims 15, 16, 19, 20, and 21, these claims recite the same limitation as claims 8, 9, 11, 12, and 13 respectively except for incorporating the claimed method into a computer program. **Porras et al** discloses implementing the invention into a computer readable medium containing instructions (see page 8, paragraph 81). Therefore, claims 15, 16, 19, 20, and 21, are rejected on the same rationale as the rejection of claims 8, 9, 11, 12, and 13.

As per claim 18, **Porras et al** discloses *wherein instructions to indicate further comprise instructions to issue an alert if the new service is detected* (see page 7, paragraph 71).

Claim Rejections - 35 USC § 103

3. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

Claims 10, 14, 17, and 22 are rejected under 35 U.S.C. 103(a) as being unpatentable over US Patent Publication 2004/0010718 to **Porras et al.**

As per claim 10, **Porras et al** substantially discloses determining whether the activity exceeds a threshold value when the entity is using a new service (unknown port) and if the threshold exceeds and the entity is using a new service, anomaly is detected (see page 4, paragraphs 47 and 48). **Porras et al** suggests using a countermeasure response to report the anomaly (see pages 6-7, paragraphs 67 and 71). Although not using the same terms as the claim language it is apparent to one of ordinary skill in the art of intrusion detection that a rule for issuing an alert may be defined as exceeding a threshold value which indicates an attack as disclosed **Porras et al** and producing a countermeasure response or reporting the attack in response to detecting can be reasonably interpreted as generating an alert. As known in the art, in an attack-response method when an attack is detected according to a specified rule, an alert is generated. Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to issue an alert if is determined whether a rule specifies to issue an alert

if the entity is providing or using the new service; and if it is also determined that the entity is providing or using the new service so as to protect the network from more global attacks by taking further actions (see page 7, paragraph 68) or by alerting other entities (see page 2, paragraph 16) as suggested by **Porras et al**.

As per claim 14, **Porras et al** substantially discloses measuring network connections and using a statistical profile to make the comparison (see page 1, paragraph 1-2) but does not explicitly disclose that the statistical profile is represented as a connection table. Examiner takes official notice that it is very well known in the art that network events can be represented in a form of a table and it would have been obvious to one of ordinary skill in the art at the time the invention was made to modify the statistical profile of measures of network connections of **Stewart et al** and implement it in a connection table so as to make it easier for reading, editing, and interpreting the data as known in the art.

As per claim 17, **Porras et al** substantially discloses determining whether the activity exceeds a threshold value when the entity is using a new service (unknown port) and if the threshold exceeds and the entity is using a new service, anomaly is detected (see page 4, paragraphs 47 and 48). **Porras et al** suggests using a countermeasure response to report the anomaly (see pages 6-7, paragraphs 67 and 71). Although not using the same terms as the claim language it is apparent to one of ordinary skill in the art of intrusion detection that a rule for issuing an alert may be defined as exceeding a threshold value which indicates an attack as disclosed **Porras et al** and producing a countermeasure response or reporting the attack in

response to detecting can be reasonably interpreted as generating an alert. As known in the art, in an attack-response method when an attack is detected according to a specified rule, an alert is generated. Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to issue an alert if is determined whether a rule specifies to issue an alert if the entity is providing or using the new service so as to protect the network from more global attacks by taking further actions (see page 7, paragraph 68) or by alerting other entities (see page 2, paragraph 16) as suggested by **Porras et al**.

As per claim 22, **Porras et al** substantially discloses collecting statistical measures to provide the most recent data represented as short-term statistical profiles (current list) and the normal, non-recent, data as long-term statistical profiles (baseline list) (see page 1, paragraph 1-2, paragraphs 11 and 15, page 3, paragraphs 33 and 36 and page 4, paragraph 40), but does not explicitly state that the statistical measures are represented in a table. Examiner takes official notice that it is very well known in the art that network events can be represented in a form of a table and it would have been obvious to one of ordinary skill in the art at the time the invention was made to modify the statistical profile of measures of network connections of **Stewart et al** and implement it in a connection table so as to make it easier for reading, editing, and interpreting the data as known in the art.

4. **Claims 1-7** are rejected under 35 U.S.C. 103(a) as being unpatentable over US Patent Publication 2004/0010718 to **Porras et al** in view of US Patent 7,047,288 to **Cooper et al**.

As per claim 1, **Porras et al** substantially discloses a graphical user interface (see page 3, paragraph 31) for configuring a new service detection process, and discloses tracking an entity in the network (see page 1, paragraph 11) a method that allows a system to track *if the selected entity is providing or consuming a service* (such as using unknown port protocol) (see pages 4-5, paragraphs 40-41, 47-48); *depicts a range over which to track the selected entity* (see page 3, paragraph 35); *specifying severity for an alert generated if a new service is detected* (see pages 4-5, paragraphs 41 and 47-48; and pages 6-7, paragraph 67). **Porras et al** does not explicitly disclose the details of the graphical user interface. However, it would have only required routine skill in the art to implement the steps above into fields in a graphical user interface to make it interactive. **Cooper et al** in an analogous art teaches generating a human readable English language description of a formal specification of network security policy that allows non-technical user within a user's organization to comprehend the policy by making the description simple enough to understood (see abstract). **Cooper et al** discloses a graphical user interface (see for instance fig. 9) that includes several fields including field for specifying a host name, field for service being tracked (see figs. 9 and 31) that meets the recitation of *a first field that depicts choices for entities to track in the network*, field for specifying a range of the entity being tracked (see column 13, lines 25-67 and fig. 9) and field specifying a severity for an alert generated (see fig. 9). Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to modify **Porras et al** to implement the method disclosed by **Porras et al** into a graphical user interface represented by fields as disclosed in **Cooper et al**. One of ordinary skill in the art would have been recognized the advantages disclosed by **Cooper et al** who teaches generating a human readable English language description of a formal

specification of network security policy that allows non-technical user within a user's organization to comprehend the policy by making the description simple enough to understood (see abstract).

As per claim 2, the references as combined above disclose *wherein the fields are linguistically tied together on the interface to form a sentence that corresponds to a rule* (see **Cooper et al**, column 28, lines 10-51 and fig. 12). Claim 2 is therefore rejected on the same rationale as the rejection of claim 1 above.

As per claim 3, the references as combined above disclose updating new rules in a database that meets the recitation of a list of new service detection rules stored in the detection system (see **Cooper et al**, column 68, lines 14-67). Claim 3 is therefore rejected on the same rationale as the rejection of claim 1 above. Claim 4 is therefore rejected on the same rationale as the rejection of claim 1 above.

As per claim 4, the references as combined above disclose a field that allows a user to specify the entity to track as *a specific host, any host in a specific role, any host in a specific segment, or any host* (see **Porras et al,** page 1, paragraph 10 and **Cooper et al**, fig. 31 and fig. 9).

As per claim 5, the references as combined above disclose a field that specifies details for the extent of the comparison for the entity specified in the first field as *host, in its role, in its*

segment or anywhere in the network (see **Cooper et al**, figs. 9, 10C, and 31). Claim 5 is therefore rejected on the same rationale as the rejection of claim 1 above.

As per claim 6, the references as combined above disclose the claimed method of claim 1. **Porras et al** also discloses wherein event severity is a numerical value (see **Porras et al,** page 6, paragraph 67) and **Cooper et al** discloses a graphical interface for entering severity value (see **Cooper et al**, fig. 9). Claim 6 is therefore rejected on the same rationale as the rejection of claim 1 above.

As per claim 7, the references as combined above disclose the claimed method of claim 1. **Cooper et al** further discloses pull down menu for inputting the information in the fields (see fig. 31). Claim 7 is therefore rejected on the same rationale as the rejection of claim 1 above.

Conclusion

5. **THIS ACTION IS MADE FINAL.** Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the mailing date of this final action.

5.1 The prior art made of record and not relied upon is considered pertinent to applicant's disclosure as the prior art discloses several of the claimed features such as graphical user interface for implementing network detection and comparing recent event detection with known event to determine that new service is detected. (See PTO-form 892).

5.2 Any inquiry concerning this communication or earlier communications from the examiner should be directed to CARL COLIN whose telephone number is (571)272-3862. The examiner can normally be reached on Monday through Thursday, 8:00-6:30 PM.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Nasser G. Moazzami can be reached on 571-272-4195. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

/Carl Colin/
Primary Examiner, Art Unit 2136
June 21, 2008